

## INFORMATION TECHNOLOGY

Information technology (IT) is an indispensable tool of modern government and one in which the State has invested heavily. When the statutory authorization for the Department of Information Technology (DOIT) sunset in July 2002, the Administration and Legislature agreed that major reforms were needed to achieve effective statewide planning for and management of information technology.

### Information Technology Governance in Transition

- ◆ The Legislature preserved funding in the budget for two core activities—oversight and security—providing \$2 million to the Department for Finance (Finance) for these purposes. The Administration therefore began the 2002-03 fiscal year with three tasks: create an interim IT governance structure during the transition until a new statutory framework could be adopted effective January 1, 2004; implement oversight and security programs that worked; and propose a permanent plan to the Legislature for IT governance.



- ◆ In May 2002, the Administration directed state agencies in Executive Order D-57-02 to implement IT management reforms. The Administration also appointed a State Chief Information Officer (CIO) within the Governor's Office to coordinate the control agencies and departments that have lead IT responsibilities and to provide leadership on statewide IT issues. These efforts resulted in a collaborative governance model that is neither centralized nor decentralized. Finance, with the guidance of the State CIO, is the control agency most directly accountable for ensuring that the fundamentals of IT governance are met during this transition period.
- ◆ In developing an oversight program, Finance has defined project oversight, assigned broad roles building on the direction provided in the Executive Order, and is currently developing a framework for project reviews and reporting. Project oversight identifies and quantifies any issues and risks affecting project components and implements appropriate remediation plans for the identified project risks.
- ◆ In developing a statewide security program, Finance reached out to key partner agencies for planning assistance, creating an interagency "community" approach to a security program. This approach relies on clear definition of roles and wise use of the existing resources to create an informed community of state IT professionals who focus on mitigating the highest IT security risks.
- ◆ The critical next steps for security include: identifying existing statewide security resources and authorities; implementing a security communication plan; beginning risk identification; improving security awareness and knowledge; managing security incidents; and establishing the confidentiality of security information.



---

## New Statutory Framework for Information Technology Governance

- ◆ The first step towards a permanent governance structure is to build consensus on a broad vision for the use of information technology in state operations and on basic governance principles that guide the State towards that vision. A working vision is: *The State will manage, deploy, and develop its information technology resources to support responsive and cost-effective state operations, and to establish timely and convenient delivery of state services, benefits, and information.*
- ◆ The Administration believes that effective statewide management of IT is based on clear strategic thinking, sound management of the existing IT operations, and demonstrated accountability. The future governance structure needs to address all three requirements. In particular, public trust in the State's IT governance needs to be restored.
- ◆ Basic governance principles will guide the State towards a new governance structure. These principles include the following:
  - ◇ Strategic planning must address both current and anticipated needs, and there must be a bridge between strategic decision-making and operational activity.
  - ◇ Sound administration is based on assigning governance tasks by expertise: service agencies primarily have operational responsibility, control agencies have oversight responsibilities, and the CIO should remain primarily at the strategic level. An Information Technology Board could provide a public forum for coordination and the highest level of IT program oversight.



- ◇ The responsibility for ensuring compliance with state policy and procedure must be embraced at each level of governance: project managers, department Information Security Officers, department Chief Information Officers, department directors, agency secretaries, Department of General Services, Finance, and the State CIO.
- ◆ By February 1, 2003, the Administration will provide a specific proposal and draft legislation for a permanent IT governance structure that is based on the fundamental principles above.

